WHAT IS CLAIMED IS:

1. A method for monitoring cryptographically protected data being transmitted between a client and a target server via a monitoring server, the method comprising the steps of:

exchanging information between the client and the target server to enable the cryptographically protected data to be created and read as decoded cryptographically protected data at both the client and the target server;

sending to the monitoring server enabling data associated with the information exchanged between the client and the target server, the enabling data enabling the monitoring server to read the cryptographically protected data transmitted through the monitoring server as the decoded cryptographically protected data;

analyzing the decoded cryptographically protected data at the monitoring server for determining if the non-cryptographically protected data is suspect data; and

at times when the monitoring server determines that the decoded cryptographically protected data is suspect data preventing the transmission of the cryptographically protected data between the client and the target server.

2. A method as recited in claim 1, wherein the information exchanged between the client and the target server results in the client and target server using a common ciphersuite and a common set of ciphersuite keys for creating the cryptographically protected data and reading the cryptographically protected data as decoded cryptographically protected data.

3. A method as recited in claim 2, wherein the enabling data identifies the common ciphersuite and provides the monitoring server with the ability to obtain the common set of ciphersuite keys.

4. A method as recited in claim 2, wherein the enabling data identifies the common ciphersuite and provides the monitoring server with a subset of the common set of ciphersuite keys.

5. A method as recited in claim 4, wherein having the subset of the common set of ciphersuite keys and the ciphersuite provides the monitoring server with the ability to read any of the cryptographically protected data created at the client and sent to the target server via the monitoring server but does not provide the monitoring server with the ability to read cryptographically protected data created at the target server and sent to the client via the monitoring server.

6. A method as recited in claim 1, further comprising storing the suspect data for future analysis.

7. A method as recited in claim 6, wherein the contents of the decoded cryptographically secure data is analyzed at the monitoring server and determined to be suspect data if the contents include data that has previously been identified as not being appropriate for transmission between the client and the target server.

8. A method as recited in claim 6, wherein the contents of the decoded cryptographically secure data is analyzed at the monitoring server and determined to be suspect data if it includes any known viruses.

9. A method as recited in claim 1, wherein the exchanging of information between the client and target server establishes an SSL communication session between the client and target server.

10. A method as recited in claim 9, wherein the client and monitoring server are implemented as part of a private corporate network.

11. A monitoring system for a corporate network comprising:

a client that exchanges information with a target server to establish an SSL communication channel through which cryptographically protected data is exchanged between the client and the target server using an SSL protocol; and

a monitoring server through which the cryptographically protected data is routed as part of its exchange between the client and the target server;

wherein the client sends enabling data to the monitoring server that enables the monitoring server to read the cryptographically protected data received at the monitoring server as decoded cryptographically protected data, the monitoring server analyzes the decoded cryptographically protected data to determine if it is suspect data, and at times when the monitoring data determines that the decoded cryptographically protected data is suspect data the monitoring server prevents the transmission of the cryptographically protected data between the client and the target server.

12. A monitoring system as recited in claim 11, wherein the establishment of the SSL communication channel results in the client and target server using a common ciphersuite and a common set of ciphersuite keys for creating the cryptographically protected data and reading the cryptographically protected data as decoded cryptographically protected data.

13. A monitoring system as recited in claim 12, wherein the enabling data identifies the common ciphersuite and provides the monitoring server with the ability to obtain the common set of ciphersuite keys.

14. A monitoring system as recited in claim 12, wherein the enabling data identifies the common ciphersuite and provides the monitoring server with a subset of the common set of ciphersuite keys.

15. A monitoring system as recited in claim 14, wherein having the subset of the common set of ciphersuite keys and the ciphersuite provides the monitoring server with the ability to read any of the cryptographically protected data created at the client and sent to the target server via the monitoring server but does not provide the monitoring server with the ability to read cryptographically protected data created at the target server and sent to the client via the monitoring server.

16. A monitoring system as recited in claim 11, further comprising means for storing the suspect data.

17. A monitoring system as recited in claim 11, wherein the decoded cryptographically secure data is considered to be the suspect data if it includes any known viruses.

18. A monitoring system as recited in claim 11, wherein the decoded cryptographically secure data is considered to be the suspect data if it includes data that has been pre-designated as being inappropriate for transmission between the client and the target server.

19. A method as recited in claim 11, wherein the data that has been pre-designated as being inappropriate for transmission between the client and the target server is confidential or proprietary information.

20. A method for monitoring cryptographically protected data being transmitted between a client and a target server via a monitoring server, the method comprising the steps of:

exchanging information between the client and the target server to enable the cryptographically protected data to be created and read as decoded cryptographically protected data at both the client and the target server;

sending to the monitoring server enabling data associated with the information exchanged between the client and the target server, the enabling data enabling the monitoring server to read the cryptographically protected data transmitted through the monitoring server as the decoded cryptographically protected data;

analyzing the decoded cryptographically protected data at the monitoring server for determining if the decoded cryptographically protected data is suspect data; and

at times when the monitoring server determines that the decoded cryptographically protected data is suspect data storing the suspect data and allowing the transmission of the cryptographically protected data between the client and the target server.